LIQUIDITY.IO

The Liquidity Network

A Regulated Securities Settlement Blockchain

Zach Kelling

Satschel, Inc.

Version 1.0 — April 2026

Chain ID 8675309 · Quasar Consensus · 204ms Finality
NIST PQ Crypto (FIPS 203/204/205) · Native DEX Precompiles
MPC Custody · FHE Confidential Trading · T+0 Settlement

Contents

Abstract

The Liquidity Network is a sovereign EVM Layer 1 blockchain purpose-built for regulated securities settlement. Operating at chain ID 8675309, it combines Quasar consensus—a metastable BFT protocol descended from HotStuff—with post-quantum cryptographic signatures, native DEX precompiles, MPC custody, and fully homomorphic encryption to deliver institutional-grade securities infrastructure with T+0 settlement finality.

This paper describes the architecture, consensus mechanism, cryptographic primitives, regulatory framework, and economic model of the Liquidity Network as deployed for the Liquidity.io Alternative Trading System (ATS), a FINRA-registered broker-dealer and SEC-registered transfer agent operated by Satschel, Inc.

Introduction

Traditional securities settlement operates on a T+1 cycle (reduced from T+2 in May 2024), involving a chain of intermediaries: executing brokers, clearing firms, the DTCC, custodian banks, and transfer agents. Each intermediary adds latency, cost, and counterparty risk. A single equity trade touches six or more entities before settlement is final.

The Liquidity Network eliminates this intermediary chain by embedding settlement, custody, compliance, and transfer agency directly into the blockchain protocol layer. Securities are tokenized as ERC-3643 compliant tokens with on-chain transfer restrictions. Trades execute through native DEX precompiles at sub-microsecond latency. Settlement is atomic and final within 204ms—the time for a single Quasar consensus round.

Design Goals

1. **Regulatory compliance by construction**: KYC/AML, accreditation, jurisdiction checks enforced at the protocol level, not the application level.
2. **Post-quantum security**: All consensus signatures use NIST FIPS 203/204/205 lattice-based cryptography; no reliance on elliptic curves for long-term security.
3. **Institutional custody**: CGGMP21 + FROST threshold MPC with HSM-backed shards; no single point of key compromise.
4. **Confidential trading**: FHE-encrypted order books and dark pool matching prevent information leakage and front-running.
5. **Sub-microsecond execution**: GPU-accelerated matching via native EVM precompiles; no smart contract interpretation overhead.
6. **Atomic settlement**: Trade execution and ownership transfer occur in the same transaction—no clearing cycle.

Network Architecture

Chain Parameters

Parameter	Value
Chain ID	8675309

Consensus	Quasar (metastable BFT, HotStuff lineage)
Block Time	10ms (GPU BLS), 100ms (CPU BLS fallback)
Finality	10ms deterministic (single round)
Gas Limit	1B per block (∼47,619 txs)
EVM	C++ EVM + Metal/CUDA GPU shader execution
Execution TPS	952K (C++ CPU), 47.6M (GPU)
TPS with Finality	**4.76M** (GPU BLS consensus + pipelining)
Gas Token	LQDTY
Max Validators	1,000 (permissioned set)
Min Stake	100,000 LQDTY
PQ Signatures	ML-DSA (FIPS 204) for consensus
Network Type	Sovereign L1 (Lux fork)

Node Architecture

Each Liquidity Network node runs the following components:

```
liquidityd
  |-- consensus/ Quasar BFT consensus engine
  |-- evm/ EVM execution environment
  |-- precompiles/ Native DEX, FHE, PQ precompiles
  |-- p2p/ Peer-to-peer networking (QUIC)
  |-- api/ JSON-RPC + WebSocket + FIX 4.4
  |-- custody/ MPC signer co-processor
  |-- compliance/ On-chain KYC/AML oracle
  |-- indexer/ Blockscout indexer
```

Multi-Chain Topology

The Liquidity Network inherits the Lux multi-chain architecture, deploying specialized chains for distinct workloads:

Chain	**Purpose**	**VM**	**Key Precompiles**
C-Chain	EVM contracts, token issuance	EVM	DEX, FHE, PQ, Compliance
D-Chain	Native DEX matching	DEX VM	PoolManager, CLOB, Oracle
Blockscout	GraphQL read index	Blockscout	Read-only queries
Liquid Threshold	Key management, MPC	Threshold VM	PQ KMS, Threshold, FHE
P-Chain	Validator management	Platform VM	Staking, Rewards

Quasar Consensus

The Liquidity Network uses Quasar [2], a BFT consensus protocol descended from HotStuff [3]. Quasar achieves single-round deterministic finality with $O(n)$ message complexity, pipelined voting, and dual-certificate finality. The full protocol specification, safety proofs, and scaling benchmarks are presented in the Lux Quasar papers [2].

Key properties for the Liquidity Network:

- **204ms median finality** with 7 permissioned validators across 3 US datacenters.
- **Dual certificates**: Every block carries both a BLS12-381 aggregate signature (classical) and an ML-DSA-65 signature (post-quantum). Both must be valid for finality.

- **10,400 TPS** throughput for simple transfers; 4,800 TPS for ERC-3643 compliant security token transfers.
- **Safety**: $P(\text{violation}) < 2^{-128}$ assuming adversary controls $< 1/3$ of stake.

Post-Quantum Cryptography

The Liquidity Network deploys all three NIST post-quantum standards ratified in 2024: ML-KEM-768 (FIPS 203) for key encapsulation, ML-DSA-65 (FIPS 204) for digital signatures, and SLH-DSA (FIPS 205) for cold storage. The implementation details, hybrid signature construction, and performance benchmarks are presented in the Lux PQ paper [4].

Liquidity Network specifics:

- **Hybrid transaction signatures**: secp256k1 ECDSA (EVM compatibility) + ML-DSA-65 (PQ security). The EVM validates ECDSA; the consensus layer validates both.
- **Hybrid key exchange**: X25519 + ML-KEM-768 for node-to-node QUIC transport, providing forward secrecy against both classical and quantum adversaries.
- **Dual-certificate consensus**: Every finalized block carries both a BLS and an ML-DSA aggregate certificate (see Section 4).

Native DEX Precompiles

Architecture

The Liquidity Network embeds exchange matching logic directly into the EVM as native precompiled contracts. This eliminates smart contract interpretation overhead, achieving sub-microsecond order matching latency.

Precompile	Address	LP Spec	Function
PoolManager	0x...9010	LP-9010	Pool creation, liquidity management
OracleHub	0x...9011	LP-9011	TWAP, VWAP, volatility oracles
SwapRouter	0x...9012	LP-9012	Multi-hop swap execution
HooksRegistry	0x...9013	LP-9013	Pre/post-swap hook dispatch
FlashLoan	0x...9014	LP-9014	Atomic flash loans
CLOB	0x...9020	LP-9020	Central limit order book
Vault	0x...9030	LP-9030	Yield vault management
PriceFeed	0x...9040	LP-9040	Aggregated price feeds

Performance Characteristics

Metric	Value
Order matching latency	$<1\mu$s (precompile) vs $\sim$500μs (Solidity)
Gas cost (swap)	21,000 (native) vs $\sim$150,000 (Uniswap V3)
Max orders per block	10,000
Pool types	AMM (constant product, concentrated), CLOB, RFQ

CLOB Precompile (LP-9020)

The CLOB precompile implements a price-time priority order book directly in compiled Go, bypassing the EVM interpreter entirely. Orders are stored in a red-black tree keyed by price level, with FIFO queues at each level.

```
// Solidity interface
interface ICLOB {
    function placeLimitOrder(
        address token0, address token1,
        bool isBuy, uint256 price, uint256 quantity
    ) external returns (bytes32 orderId);

    function cancelOrder(bytes32 orderId) external;

    function getOrderBook(address token0, address token1, uint8 depth)
        external view returns (PriceLevel[] bids, PriceLevel[] asks);
}
```

MPC Custody

Threshold Signature Schemes

The Liquidity Network deploys two complementary MPC protocols for non-custodial key management:

Protocol	Curve	Threshold	Use Case
CGGMP21 [9]	secp256k1 (ECDSA)	t-of-n	EVM transaction signing
FROST [10]	ed25519 (Schnorr)	t-of-n	Consensus validator signing

Shard Distribution

For institutional accounts, the default configuration is 2-of-3 threshold:

```
Shard 1: User device (biometric-gated, Secure Enclave/TPM)
Shard 2: Liquidity.io ATS co-signer (rate-limited, policy-enforced)
Shard 3: HSM escrow (third-party custodian, disaster recovery)

Signing: User + ATS (normal operations)
Recovery: User + Escrow (ATS cannot unilaterally move funds)
```

Policy Engine

The ATS co-signer enforces configurable policies before co-signing any transaction:

- **Rate limits**: Maximum transaction value per hour/day
- **Whitelist**: Destination address must be on approved list
- **Compliance**: Transaction must pass real-time AML screening
- **Settlement window**: Securities can only transfer during market hours
- **Lockup**: Rule 144 restricted securities cannot transfer before lockup expiry

FHE Confidential Trading

Motivation

Public blockchains expose all transaction data, creating front-running, sandwich attacks, and information leakage. For regulated securities—where material non-public information (MNPI) and block trade disclosure are governed by SEC rules—on-chain transparency is a regulatory liability.

FHE Schemes

Scheme	Operations	Use Case
TFHE	Boolean/integer arithmetic	Dark pool order matching
CKKS	Approximate real arithmetic	Portfolio analytics, risk computation

Dark Pool Architecture

Orders submitted to the Liquidity.io dark pool are encrypted client-side using TFHE:

1. Trader encrypts order (side, price, quantity) with the network's collective FHE public key.
2. Encrypted order is submitted to the D-Chain matching engine.
3. The matching engine operates on encrypted values—comparing prices and matching quantities without decryption.
4. Matched orders produce an encrypted settlement instruction.
5. A threshold decryption committee (Liquid Threshold validators) decrypts only the settlement output.
6. Settlement executes on C-Chain, transferring tokens atomically.

Unmatched orders are never decrypted. No validator, node operator, or network participant can observe order flow.

Regulatory Framework

Registration Status

Entity	Registration	Regulator
Satschel, Inc.	Broker-Dealer (BD)	FINRA / SEC
Satschel, Inc.	Alternative Trading System (ATS)	SEC (Reg ATS)
Satschel, Inc.	Transfer Agent (TA)	SEC

On-Chain Compliance Enforcement

The Liquidity Network enforces regulatory requirements at the protocol level through a Compliance Oracle precompile:

- **KYC/AML**: Every address must be KYC-verified before receiving security tokens. The Compliance Oracle maintains an on-chain identity registry keyed by address.
- **Accredited Investor**: Reg D 506(c) securities require accredited investor verification. The oracle stores accreditation status with expiry dates.

- **Jurisdiction**: Transfer restrictions by jurisdiction (e.g., no transfers to OFAC-sanctioned countries).
- **Holding Period**: Rule 144 lockup periods enforced at the token level—transfers revert if the lockup has not expired.
- **Maximum Holders**: Reg D 506(b) limits to 35 non-accredited investors per offering.

T+0 Settlement

On the Liquidity Network, trade execution and settlement occur in the same transaction:

```
Traditional: Trade -> Clear -> Settle (T+1, ~26 hours)
Liquidity: Trade + Settle (T+0, ~204ms consensus finality)
```

This eliminates:

- Counterparty risk during the settlement window
- Failed trade risk (currently 1–3% of equity trades)
- Capital locked as margin during settlement
- The DTCC, NSCC, and DTC intermediary chain

USDL Stablecoin

Settlement on the Liquidity Network is denominated in USDL, a fiat-backed stablecoin:

Property	Value
Name	USDL (USD Liquidity)
Type	ERC-20 with transfer restrictions
Backing	1:1 USD in segregated bank accounts
Attestation	Monthly proof-of-reserves by independent auditor
Redemption	T+0 for qualified participants

Economic Model

LQDTY Token

LQDTY is the native gas token of the Liquidity Network, used for transaction fees, validator staking, and governance.

Parameter	Value
Total Supply	1,000,000,000 LQDTY
Initial Circulating	100,000,000 LQDTY (10%)
Validator Stake Minimum	100,000 LQDTY
Block Reward	2 LQDTY (decreasing annually)
Fee Model	EIP-1559 base fee + priority fee
Fee Burn	50% of base fee burned

Fee Structure

Operation	Fee (LQDTY)	Fee (USD equiv.)

Token transfer	0.001	∼$0.001
Security token trade	0.01	∼$0.01
Pool creation	1.0	∼$1.00
Security issuance	100.0	∼$100

Trading fees on the DEX are separate from gas fees and configurable per pool (default 30bps for securities, 5bps for stablecoins).

Validator Economics

Validators earn block rewards plus a share of trading fees proportional to their stake. The minimum hardware requirements ensure network performance:

Requirement	**Specification**
CPU	16 cores (AMD EPYC or Intel Xeon)
RAM	64 GB
Storage	2 TB NVMe SSD
Network	10 Gbps dedicated
GPU (optional)	NVIDIA A100 (for FHE acceleration)

Conclusion

The Liquidity Network represents a fundamental rearchitecture of securities settlement infrastructure. By embedding compliance, custody, matching, and settlement directly into the blockchain protocol layer—and securing it with post-quantum cryptography and fully homomorphic encryption—the network eliminates the intermediary chain that has defined capital markets infrastructure for decades.

The result is a regulated, compliant, and cryptographically secure settlement layer that achieves T+0 finality in 204ms, reduces settlement costs by orders of magnitude, and provides institutional-grade custody without centralized key management.

Built on the open source Lux Network foundation, the Liquidity Network inherits a battle-tested codebase while extending it with the specialized precompiles, compliance oracles, and confidential computing capabilities required for regulated securities markets.

References

[1] Z. Kelling, “Lux Consensus: A Scalable BFT Protocol for Multi-Chain Networks,” Lux Partners, 2023.

[2] Z. Kelling, “Quasar: Post-Quantum Metastable Consensus Descended from HotStuff,” Lux Partners, 2024.

[3] M. Yin, D. Malkhi, M. K. Reiter, G. Golan-Gueta, I. Abraham, “HotStuff: BFT Consensus with Linearity and Responsiveness,” PODC, 2019.

[4] Z. Kelling, “Post-Quantum Cryptography for Blockchain Consensus,” Lux Partners, 2024.

[5] Z. Kelling, "Lux DEX: Native EVM Precompiles for Sub-Microsecond Order Matching," Lux Partners, 2024.

[6] Z. Kelling, "Non-Custodial MPC Custody Architecture for Digital Securities," Lux Partners, 2025.

[7] Z. Kelling, "FHE Dark Pools: Confidential Order Matching on Public Blockchains," Lux Partners, 2025.

[8] Z. Kelling, "Liquidity.io Full Stack Architecture," Satschel, Inc., 2026.

[9] R. Canetti, R. Gennaro, S. Goldfeder, N. Makriyannis, U. Peled, "UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts," ACM CCS, 2020.

[10] C. Komlo, I. Goldberg, "FROST: Flexible Round-Optimized Schnorr Threshold Signatures," SAC, 2020.

[11] NIST, "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)," 2024.

[12] NIST, "FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)," 2024.

[13] NIST, "FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)," 2024.

[14] Tokeny, "ERC-3643: T-REX Token for Regulated Exchanges," Ethereum, 2021.

[15] V. Buterin et al., "EIP-1559: Fee Market Change for ETH 1.0 Chain," Ethereum, 2021.

[16] SEC, "Regulation ATS: Alternative Trading Systems," 17 CFR 242.300–303, 1998.

[17] SEC, "Rule 144: Selling Restricted and Control Securities," 17 CFR 230.144, 1972 (amended 2008).

The Liquidity Network is built on open source technology from the Lux Network ecosystem.
All upstream Lux repositories are open source (BSL-1.1, MIT, Apache-2.0).

Lux Platform Specs (LPs): https://github.com/luxfi/lps